

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

FILED**APR 05 2019**UNDER SEALMAGISTRATE JUDGE SUSAN E. COX
UNITED STATES DISTRICT COURT

In the Matter of the Search of:

Case Number: 16 CR 793

The Mailgun Technologies, Inc. account
admin@digitallydirectmktng.com, further described in
Attachment A

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Michael C. Devine, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Western District of Texas, there is now concealed:

See Attachment A, Part III

The basis for the search under Fed. R. Crim. P. 41(c) is evidence and instrumentalities.

The search is related to a violation of:

*Code Section**Offense Description*

Title 18, United States Code, Section 1030

computer fraud

Title 18, United States Code, Section 1037

illegal spamming

Title 18, United States Code, Section 1343

wire fraud

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.

*Applicant's Signature*MICHAEL C. DEVINE, Special Agent
Federal Bureau of Investigation*Printed name and title*

Sworn to before me and signed in my presence.

Date: April 5, 2019*Judge's signature*City and State: Chicago, IllinoisSUSAN E. COX, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS) ss:

AFFIDAVIT

I, Michael C. Devine, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately June 2016.

2. As part of my duties as a Federal Bureau of Investigations Special Agent, I investigate criminal violations relating to federal criminal offenses. I specialize in the investigation of computer and high-technology crimes, including complex computer intrusions, denial of service attacks, and other types of malicious computer activity. During my career as an FBI Special Agent I have participated in numerous cyber-related investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. I have participated in the execution of numerous federal search warrants.

3. This affidavit is made in support of an application for a warrant to search, pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with an account that is stored at the premises owned, maintained, controlled, or operated by Mailgun Technologies, Inc. ("Mailgun"), a free web-based electronic mail service provider located at 112 E. Pecan St. #1135, San Antonio, Texas 78205. The account to be searched is admin@digitallydirectmktng.com (hereinafter, the "**Subject Account**"), which is

further described in the following paragraphs and in Part II of Attachment A. As set forth below, there is probable cause to believe that in the account, described in Part II of Attachment A, in the possession of Mailgun, there exists evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer fraud), 1037 (illegal spamming), and 1343 (wire fraud) (the “**Subject Offenses**”).

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of the **Subject Offenses** are located in the **Subject Account**.

BACKGROUND INFORMATION

Mailgun Technologies, Inc.

5. Based on my training and experience, I have learned the following about Mailgun:

a. Mailgun is an e-mail automation engine used by developers for sending, receiving, and tracking e-mails. Subscribers obtain an account by registering on the Internet with Mailgun. Mailgun requests subscribers to provide basic

information, such as a name, a name for the associated business or company, a business e-mail address, and payment information;

b. Mailgun maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records often include account access information, e-mail transaction information, and account application information;

c. The content of any e-mail that is sent from a Mailgun subscriber is stored on a Mailgun controlled server for a period of three days. E-mail metadata, subject line data, and delivery information is also stored on a Mailgun controlled server for a period of 30 days.

d. Mailgun is a unique method to distribute a large volume of e-mail because it uses a hypertext transfer protocol application programming interface (HTTP API) rather than simple mail transfer protocol (SMTP). SMTP is the most commonly used protocol for transferring e-mail. Most major businesses send and receive e-mail through SMTP via their own unique domain name. Also, commonly used web-based e-mail providers such as Gmail and Yahoo! Mail use SMTP to send and receive user e-mails. Using HTTP API instead of SMTP is beneficial to a Mailgun subscriber if he/she is using a server that does not support SMTP or where SMTP is restricted, and is faster and more efficient based on the Mailgun homepage.

**FACTS SUPPORTING PROBABLE CAUSE TO
SEARCH THE SUBJECT ACCOUNT**

Background on Spam

6. Based on my training, experience, knowledge, and conversations with other experienced law enforcement personnel, I know the following:

a. Spam:

i. As used in this affidavit, “spam” refers to unsolicited bulk e-mail. “Unsolicited” means that the recipient has not granted deliberate and revocable permission for the e-mail to be sent to him or her. “Bulk” means that the e-mail was sent as part of a larger collection of e-mails, which have substantively identical content. The content of spam varies, but does not affect its classification as spam so long as the e-mail is unsolicited and bulk.

ii. Typically, spam is commercial in nature and used by unregulated online retailers to advertise and mass-market unregulated or counterfeit products directly to consumers.

iii. A spam “affiliate program” is a type of business or online retailer – such as an Internet pharmacy – that pays a third party, known as “affiliates” or “spammers,” a percentage of any sales that they generate for the program. Affiliates or spammers typically generate sales by sending spam that contains hyperlinks to hundreds or thousands of e-mail addresses. A “hyperlink” re-directs the e-mail recipient’s computer Internet browser program to the affiliate program’s website on the Internet. In some instances, the hyperlinks can contain computer viruses and other forms of malicious software or “malware.”

iv. Spammers use “mass e-mail software” or “spamming software” to generate, send, and automate spam. Depending on the number of computers used to send spam, spamming software can send over two million e-mails in just ten minutes. Spammers also use multiple domain names in order to enable mass mailings by increasing the number of e-mail domains used to send spam simultaneously. As of 2013, more than 68 percent of all e-mail sent worldwide was spam.

b. The Adverse Effects of Spam on Host Companies:

i. A “web hosting company” or a “host company” is a type of company that leases server space on a private network in exchange for a fee. These companies usually provide servers (of varying kinds), data storage, network access, as well as connections to the Internet, typically in a data center. The scope of web hosting services or plans vary and is typically based on a service contract.

ii. Unlike traditional print unsolicited bulk mail, where the costs of printing and postage are borne by the sender, spam imposes significant costs on its recipients and the computer networks used to transmit spam. In short, spam is unwanted and useless data that is transmitted and stored on servers and networks that are owned and maintained by third-parties (such as host companies), that are forced to bear the costs of storing and delivering spam.

iii. Spam can overload servers and networks, delay data transmissions, and cause system outages. Spam increases the traffic of e-mails and

other data processed on different servers and, as a result, delays and can prevent the delivery of legitimate e-mail and data. If the volume of spam exceeds the capacity of a server or network, the result is a system outage. As a result, host companies may be forced to purchase new hardware, software, and bandwidth, among other things, in response to spam. According to one U.S.-based ISP, spam imposes approximately \$1 million per month in costs.

iv. Spam can also cause disruptions to service when a host company's internet protocol ("IP") addresses are "blacklisted" because the IP addresses are identified as a source of spam. This is typically the result of a customer violating the host company's terms of service. These "blacklists," like Spamhaus Block List ("SBL"), are systems that are created to identify known sources of spam.¹ These lists are compiled so that a spam filer can check an incoming e-mail message against a database of spam sources, and block an incoming e-mail or transmission from those known sources of spam. If a host company's IP addresses are blacklisted, e-mails sent from those IP addresses may not be delivered to the intended recipient, including non-spam e-mails sent from law-abiding Internet users.² If left unresolved, additional

¹ According to their website, [www. Spamhaus.org](http://www.Spamhaus.org), Spamhaus is an "international nonprofit organization that tracks spam, and related cyber threats such as phishing, malware and botnets, provides real-time actionable and highly accurate threat intelligence to the Internet's major networks, corporations and security vendors, and works with law enforcement agencies to identify and pursue spam and malware sources worldwide." Based on my training and experience and conversations with other experienced agents, I believe information sourced to Spamhaus to be reliable.

² According to the website www.spamhaus.org (checked January 14, 2019) as of January 14, 2019, the Spamhaus Blocklist is utilized to protect 3,010,390,000 user mailboxes.

IP addresses belonging to the host company can be added to the SBL. As a result, many host companies use Terms of Service Agreements (“TOSA”) and Acceptable Use Policies (“AUPs”), which govern their customers’ use of their networks and servers, and prohibit customers from sending spam over their networks.

The Investigation of PERSAUD

7. The FBI is investigating MICHAEL ALEXANDER PERSAUD, also known as “michaelp77,” “michaelp77x,” “Michael Pearson,” “Michael Prescott,” “Michael P,” and “Jeff Martinez,” for illegal spamming and using fraud to further his spamming activities.

8. Since at least November 2012, PERSAUD has used materially false and fraudulent representations to obtain access to, and use the property, namely computer networks, IP addresses, and servers, from victim host companies for the purpose of sending spam. PERSAUD used various accounts under various aliases within his control to communicate with victim host companies under false pretenses.

9. In order to obtain access to the victims’ computer networks and servers, and IP addresses, PERSAUD falsely represented to the victim host companies that he would not utilize the victims’ computer networks to send spam by agreeing to the victims’ AUP and/or TOSA, which governed a customer’s use of the victims’ networks, servers, and IP addresses, among other things. PERSAUD knew at the time he leased access to the computer networks belonging to the victim host companies that he intended to send millions of spam e-mails over their networks in violation of the

victims' AUP and TOSA. As a result of PERSAUD's fraudulent access and use of the victim's networks, certain victims, to include their servers and networks, were subsequently blacklisted.

10. In an effort to disguise his actions, PERSAUD utilized a technique known as "listwashing," which is the practice of removing complainant e-mail addresses from an illicitly gathered e-mail list, as to not draw further attention that would result in blacklisting. Based on my experience and conversations with other law enforcement, "listwashing" is consistent with a spamming practice known as "snowshoe" spamming.³ Further, when victim host companies identified PERSAUD's activities as violating the victim's AUP and TOS and subsequently terminated PERSAUD's account, PERSAUD would attempt to further victimize the victim host companies by attempting to create separate accounts under separate individual and company aliases.

11. Based on the above conduct, on or about December 9, 2016, PERSAUD was indicted by a federal grand jury in the Northern District of Illinois on ten counts of wire fraud, in violation of Title 18, United States Code, Section 1343. *See United States v. Michael Persaud*, 16 CR 793 (N.D. Ill.) (Wood, J.).⁴

³ According to Spamhaus, "snowshoers use many fictitious business names, fake names and identities . . . [and] often use anonymized or unidentifiable WHOIS [domain] records." Based on my experience and familiarity with this investigation, PERSAUD's actions when sending e-mail leasing IP addresses, and registering domains is consistent with someone involved in Snowshoe Spamming.

⁴ PERSAUD is currently released on a \$4,500 own recognizance bond and resides in Arizona. R. 15. His bond conditions include supervision by a pretrial services officer and computer monitoring, which thus requires that PERSAUD not possess or use a computer that is not

Confidential Source Identifies PERSAUD as a Spammer

12. On or about August 15, 2018, a confidential source (“CS-1”)⁵ informed law enforcement officials that he/she was in contact with PERSAUD via the Skype chat application. Although the Skype conversation was not recorded, CS-1 provided the FBI with screenshots of the conversation with PERSAUD.

13. According to CS-1:

a. CS-1 currently operates a mass e-mail distribution software company, which PERSAUD attempted to use in order to distribute pharmaceutical re-order e-mails.

b. CS-1 identified the PERSAUD Accounts due to the account being flagged for a high amount of “bounce-back” e-mails. “Bounce-back” messages occur in the form of an e-mail that is sent to the sender’s account after a message the sender attempts to send fails to deliver. This “bounce-back” e-mail is generated either by the sender’s mail server or the receiver’s mail server. CS-1 identified two separate accounts that attempted to use CS-1’s software for the pharmaceutical distribution

monitored. *Id.* On or about November 29, 2018, the pretrial services office in Arizona confirmed that PERSAUD had accessed at least two email marketing websites, but did not have the information or resources to monitor if the email marketing was in violation of federal law. R. 60. A jury trial is scheduled in this matter for August 26, 2019. R. 53.

⁵ According to CS-1’s handling agent, CS-1 began cooperating with the FBI in or around 2009, and has provided agents with background and intelligence information relevant to a range of investigations, which has been independently corroborated by law enforcement. As a result, CS-1 has proven reliable and truthful. CS-1 began cooperating with the FBI after learning that CS-1 was under investigation. As a result of CS-1’s cooperation, CS-1 received a deferred prosecution agreement as to that investigation. CS-1 later agreed to cooperate with the FBI in exchange for monetary compensation. To date, CS-1 has been paid approximately \$15,000. According to criminal history records checks, CS-1 has no prior convictions.

campaign (the "PERSAUD Accounts").⁶ These accounts were both created under the name "Michael P" from e-mail addresses michaelp77@aol.com and michaelp77x@gmail.com respectively. Further, both accounts were created from an originating IP address, 72.216.106.206 on August 6, 2018.

14. E-mail service provider records show that both michaelp77@aol.com and michaelp77x@gmail.com are registered to PERSAUD. Additionally, the FBI has executed federal search warrants for both e-mail addresses prior to the December 9, 2016 indictment of PERSAUD. In March of 2019, the FBI received internet service provider records showing that the IP address, 72.216.106.206, was assigned to PERSAUD on August 6, 2018, when both accounts were created.

15. CS-1 provided screenshots of his/her administrative control panel, which reflected the PERSAUD Accounts information. These screenshots included account information, loaded distribution lists, subscriber e-mails within each list, a

⁶ As discussed below, law enforcement officials understand that the PERSAUD Accounts belonged to PERSAUD as follows: first, the PERSAUD Accounts were created under the name "Michael P," which I understand to be MICHAEL PERSAUD. Second, according to Mailgun, the email addresses michaelp77@aol.com and michaelp77x@gmail.com were used to create the PERSAUD Accounts. According to the email service providers AOL and Google, both email addresses were registered to MICHAEL PERSAUD. Third, internet service provider records indicate that 72.216.106.206 was assigned to PERSAUD on August 6, 2018. As discussed below, the PERSAUD Accounts were created from that IP address on August 6, 2018. Fourth, according to screenshots provided by CS-1, discussed below, the PERSAUD Accounts were created by an individual with an address of "XXX5 E. VIA SOLERI DR, APT XXX1, SCOTTSDALE, ARIZONA 85251." According to internet service provider records, PERSAUD's residence is XXX5 E. VIA SOLERI DR, APT XXX1, SCOTTSDALE, ARIZONA 85251. Fifth, as discussed below, according to screenshots provided by CS-1, the PERSAUD Accounts were created by an individual using the phone number 619-XXX-0379. Based on phone records provided by AT&T, the phone number 619-XXX-0379 is registered to PERSAUD.

copy of the pharmacy e-mail campaign, and SMTP logs. The screenshots also revealed that the accounts were registered under the username and e-mail address of “admin@digitallydirectmktng.com,” with an address of “XXX5 E. VIA SOLERI DR, APT XXX1, SCOTTSDALE, ARIZONA 85251” and telephone number of 619-XXX-0379.⁷ Previously attained phone records indicated that 619-XXX-0379 is an AT&T Wireless subscriber number registered to PERSAUD. This account had an assigned domain name of webstreetinfo.com, which was created on or about August 5, 2018.

16. According to CS-1, CS-1’s software company suspended the PERSAUD Accounts due to his spamming activity and the high volume of “bounce-back” e-mails.

17. Based on a preexisting relationship between PERSAUD and CS-1, CS-1 contacted PERSAUD via Skype Chat. According to CS-1, during that conversation:

a. PERSAUD informed CS-1 that he had signed up with Mailgun directly and had not encountered any issues with Mailgun as long as he [PERSAUD] kept his “bounce-back” e-mails down.

b. CS-1 asked PERSAUD what he was mailing and PERSAUD replied that he sent pharmacy reorder lists. PERSAUD informed CS-1 that pharmacy e-mails used to do better and that he might drop them soon. PERSAUD stated that pharmacy e-mails are currently only one percent of PERSAUD’s mailing time.

⁷ PERSAUD’s home address and phone number have been partially redacted because this pleading will ultimately be in the public record.

18. PERSAUD provided CS-1 with a referral link to the Canadian Pharmacy site hosted at trustedxreward.ru. The link redirected the visitor to a separate site hosted at <https://darkpassenger.ru/?pid=3686>. PERSAUD also provided CS-1 with login credentials (a login and password). As of January 14, 2019, Spamhaus has identified Canadian Pharmacy as number one on the list of “Top 10 Worst Spammers” in the world. The list can viewed at <https://www.spamhaus.org/statistics/spammers/>.

19. According to CS-1, during their Skype conversation, CS-1 and PERSAUD also discussed differences between CS-1’s e-mail software company and Mailgun. PERSAUD expressed his preference for Mailgun because Mailgun offers 10,000 e-mails free with a \$5.00 USD fee for each additional 10,000 e-mails.

20. Based on records provided by Mailgun, PERSAUD created a Mailgun account on or about August 14, 2018 under the name “Michael Alexander” and e-mail admin@digitallydirectmktng.com. PERSAUD registered three domains with Mailgun: (1) customerorderlink.com; (2) clientorderlink.com; and (3) fnlsmls.com. Since September 14, 2018, PERSAUD sent approximately 230,000 e-mails from customerorderlink.com. Records showed that approximately 215,000 were delivered and 16,000 were “bounce-back” e-mails.

21. Mailgun records also showed multiple successful logins to the PERSAUD Accounts from a Cox Communication based IP address, 70.176.87.63.

22. According to open source records., both the webstreetinfo.com domain used by PERSAUD on CS-1's e-mail software and the customerorderlink.com domain used by PERSAUD on Mailgun's e-mail distribution platform were registered through Namecheap, a domain registration sales company as well as web-hosting service provider located in the United States.

23. Further, PERSAUD's registration e-mail for both services, admin@digitallydirectmktng.com is a Google, Inc. G Suite Basic domain that was created under contact e-mail, michaelp77x@gmail.com.

24. Based on my training and experience in other investigations, I believe that PERSAUD's recent e-mail campaign is in violation of Mailgun's terms of service policy, namely their acceptable use policy which states that "You may not use Mailgun's network or Services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including: any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations, including data protection and privacy laws relating to unsolicited commercial electronic messages; and any action which directly or indirectly results in any of our IP space being listed on any abuse database (*i.e.* Spamhaus)."

25. Further, based on the provided screen captures, PERSAUD's recent e-mail campaign also violates Mailgun's Mail Requirements, which states:

a. You must have a Privacy Policy posted for each domain associated with the mailing;

- b. You must have the means to track anonymous complaints;
- c. You must not obscure the source of your e-mail in any manner;
- d. You must post an e-mail address for complaints (such as abuse@yourdomain.com) in a conspicuous place on any website associated with the e-mail and you must promptly respond to messages sent to that address;
- e. Your intended recipients have given their consent to receive e-mail via some affirmative means, such as an opt-in procedure, and you can produce evidence of such consent within 72 hours of receipt of a request by the recipient or Mailgun;
- f. You must use reasonable means to ensure the person giving consent is the owner of the e-mail address for which the consent is given;
- g. You must include the recipient's e-mail address in the body of the message or in the "TO" line of the e-mail;
- h. You must honor revocations of consent and notify recipients of the same.

26. On or about November 29, 2018, agents served a preservation letter on Mailgun for the **Subject Account**. On or about February 1, 2019, agents served another preservation letter on Mailgun in order to extend the preservation on the **Subject Account** for an additional 90 days.

27. Based on my training and experience in other investigations, I believe that a search of email provider account contents often of individuals engaged in criminal conduct yields investigative leads relating to:

a. the identities of participants engaged in and witnesses to bulk email sent in violation of terms of service offenses;

b. the contact information of participants engaged in and witnesses to bulk email sent in violation of terms of service offenses;

c. the timing of communications among participants and other individuals involved in bulk email sent in violation of terms of service offenses;

d. the methods and techniques used in bulk email sent in violation of terms of service offenses;

e. information regarding the physical location of participants engaged in and witnesses to bulk email sent in violation of terms of service offenses.

SEARCH PROCEDURE

28. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Mailgun Technologies, Inc. to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Mailgun Technologies, Inc. personnel who will be directed to the information described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, Mailgun Technologies, Inc. employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact duplicate of all information stored in the computer accounts and files described therein;

29. Mailgun Technologies, Inc. employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

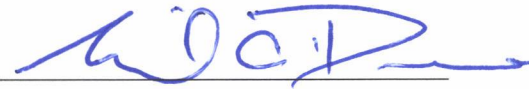
30. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records received from Mailgun Technologies, Inc. employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

CONCLUSION

31. Based on the above information, I respectfully submit that there is probable cause to believe that evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030, 1037, and 1343 are located within one or more computers and/or servers found at Mailgun Technologies, Inc., headquartered at 112

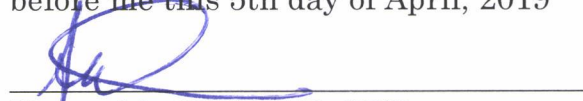
E. Pecan St. #1135, San Antonio, Texas 78205. By this affidavit and application, I request that the Court issue a search warrant directed to Mailgun Technologies, Inc. allowing agents to seize the electronic evidence and other information stored on the Mailgun Technologies, Inc. servers following the search procedure described in Attachment A and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.



Michael C. Devine
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 5th day of April, 2019


Honorable SUSAN E. COX
United States Magistrate Judge

ATTACHMENT A

I. SEARCH PROCEDURE

1. The search warrant will be presented to Mailgun Technologies, Inc. personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Mailgun Technologies, Inc. employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES OF MAILGUN TECHNOLOGIES, INC.

To the extent that the information described below in Section III is within the possession, custody, or control of Mailgun Technologies, Inc., which are stored at premises owned, maintained, controlled, or operated by Mailgun Technologies, Inc.,

headquartered at 112 E. Pecan St. #1135, San Antonio, Texas 78205, Mailgun Technologies, Inc. is required to disclose the following information to the government for the following account:

admin@digitallydirectmktng.com

c. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.

d. All electronic files stored and presently contained in, or on behalf of the account described above.

e. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.

f. All existing printouts from original storage of all the electronic mail described above.

g. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.

h. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described

above, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing and payment records.

i. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.

j. All account contents previously preserved by Mailgun Technologies, Inc., in electronic or printed form, including all e-mail, including attachments thereto, and for the account described above.

k. Pursuant to 18 U.S.C. § 2703(d), the service provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence and instrumentalities concerning violations of Title 18, United States Code, Sections 1030, 1037, and 1343 as follows:

1. Items relating to PERSAUD's use of Mailgun services;
2. Items related to PERSAUD's Mailgun account access information, e-mail transaction information, and account application information;
3. Items relating to Mailgun's terms of service policy, acceptable use policy, privacy policy, and mail requirements;

4. Items related to Canadian Pharmacy, trustedxreward.ru, and <https://darkpassenger.ru/?pid=3686>;
5. Items related to email account admin@digitallydirectmktng.com, michaelp77x@gmail.com, and michaelp77@aol.com;
6. Items related to domains customerorderlink.com, clientorderlink.com, fnlsmls.com, and webstreetinfo.com;
7. Items related to IP Address 70.176.87.63;
8. Items relating to host companies, dedicated hosting, virtual private servers, cloud based hosting and storage, and other networks used to send spam;
9. Items relating to spam, including spam emails, email logs, recipient email accounts, mass email software and other programs used to send spam, malware, proxies, false header information and other spamming tools and techniques;
10. Items relating to spam filters, Spamhaus Block List, and the CAN-SPAM Act;
11. Items relating to affiliate programs, including communications and payments;
12. Items relating to the registration of internet domains;
13. Items relating to financial transactions relating to hosting services as well as affiliate programs;
14. Items relating to the identities of affiliate programs;

15. Items relating to the use of aliases and other email accounts by PERSAUD;
16. Items relating to the timing of communications; and
17. Items relating to methods and techniques by spammers
18. Items related to the identity of the user or users of the **Subject Account**.
19. Items related to the physical location of the users of the **Subject Account** at or near the times of the **Subject Offenses**.
20. Items related to the identities and contact information of participants in or witnesses to the **Subject Offenses**.
21. All of the non-content records described above in Section II.

ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the free web-based electronic mail service provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.
- b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.
- c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or
- d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such

electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

Case Number: 16 CR 793

The Mailgun Technologies, Inc. account
admin@digitallydirectmktng.com, further described in
Attachment A

SEARCH AND SEIZURE WARRANT

To: Michael Devine and any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Texas:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

See Attachment A, Part III

YOU ARE HEREBY COMMANDED to execute this warrant on or before April 19, 2019 in the daytime (6:00 a.m. to 10:00 p.m.).

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the issuing United States Magistrate Judge.

Date and time issued: April 5, 2019 @ 2:33 pm

City and State: Chicago, Illinois



Judge's signature

SUSAN E. COX, U.S. Magistrate Judge
Printed name and title

Return

Case No:

Date and Time Warrant Executed:

Copy of Warrant and Inventory Left With:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

I. SEARCH PROCEDURE

1. The search warrant will be presented to Mailgun Technologies, Inc. personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Mailgun Technologies, Inc. employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES OF MAILGUN TECHNOLOGIES, INC.

To the extent that the information described below in Section III is within the possession, custody, or control of Mailgun Technologies, Inc., which are stored at premises owned, maintained, controlled, or operated by Mailgun Technologies, Inc.,

headquartered at 112 E. Pecan St. #1135, San Antonio, Texas 78205, Mailgun Technologies, Inc. is required to disclose the following information to the government for the following account:

admin@digitallydirectmktng.com

c. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.

d. All electronic files stored and presently contained in, or on behalf of the account described above.

e. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.

f. All existing printouts from original storage of all the electronic mail described above.

g. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.

h. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described

above, including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing and payment records.

i. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.

j. All account contents previously preserved by Mailgun Technologies, Inc., in electronic or printed form, including all e-mail, including attachments thereto, and for the account described above.

k. Pursuant to 18 U.S.C. § 2703(d), the service provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence and instrumentalities concerning violations of Title 18, United States Code, Sections 1030, 1037, and 1343 as follows:

1. Items relating to PERSAUD's use of Mailgun services;
2. Items related to PERSAUD's Mailgun account access information, e-mail transaction information, and account application information;
3. Items relating to Mailgun's terms of service policy, acceptable use policy, privacy policy, and mail requirements;

4. Items related to Canadian Pharmacy, trustedxreward.ru, and <https://darkpassenger.ru/?pid=3686>;

5. Items related to email account admin@digitallydirectmktng.com, michaelp77x@gmail.com, and michaelp77@aol.com;

6. Items related to domains customerorderlink.com, clientorderlink.com, fnlsmls.com, and webstreetinfo.com;

7. Items related to IP Address 70.176.87.63;

8. Items relating to host companies, dedicated hosting, virtual private servers, cloud based hosting and storage, and other networks used to send spam;

9. Items relating to spam, including spam emails, email logs, recipient email accounts, mass email software and other programs used to send spam, malware, proxies, false header information and other spamming tools and techniques;

10. Items relating to spam filters, Spamhaus Block List, and the CAN-SPAM Act;

11. Items relating to affiliate programs, including communications and payments;

12. Items relating to the registration of internet domains;

13. Items relating to financial transactions relating to hosting services as well as affiliate programs;

14. Items relating to the identities of affiliate programs;

15. Items relating to the use of aliases and other email accounts by PERSAUD;

16. Items relating to the timing of communications; and

17. Items relating to methods and techniques by spammers

18. Items related to the identity of the user or users of the **Subject Account**.

19. Items related to the physical location of the users of the **Subject Account** at or near the times of the **Subject Offenses**.

20. Items related to the identities and contact information of participants in or witnesses to the **Subject Offenses**.

21. All of the non-content records described above in Section II.

ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the free web-based electronic mail service provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.
- b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.
- c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or
- d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained in such

electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.